THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

	§	
LIONRA TECHNOLOGIES LIMITED,	§	
	§	
v.	§	CASE NO. 2:22-CV-322-JRG-RSP
	§	(LEAD CASE)
FORTINET, INC.	§	
	§	
	§	

CLAIM CONSTRUCTION ORDER

On November 17, 2023, the Court held a hearing to determine the proper construction of disputed terms in United States Patents No. 7,302,708, 7,685,436, 8,566,612, 7,916,630, and 7,921,323. Before the Court are the Opening Claim Construction Brief (Dkt. No. 145) filed by Plaintiff Lionra Technologies Limited ("Lionra"), the Responsive Claim Construction Brief (Dkt. No. 146) filed by Defendants Fortinet, Inc., Cisco Systems, Inc., and Palo Alto Networks, Inc. ("Defendants"), and Plaintiff's reply (Dkt. No. 148). Also before the Court are the parties' Patent Rule 4-3 Joint Claim Construction and Prehearing Statement (Dkt. No. 139) and the parties' Patent Rule 4-5(d) Joint Claim Construction Chart (Dkt. No. 149). Having reviewed the arguments made by the parties at the hearing and in their claim construction briefing, having considered the intrinsic evidence, and having made subsidiary factual findings about the extrinsic evidence, the Court hereby issues this Claim Construction Order. *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1314 (Fed. Cir. 2005) (en banc); *Teva Pharm. USA, Inc. v. Sandoz, Inc.*, 135 S. Ct. 831, 841 (2015).

Table of Contents

I. BACKGROUND

Plaintiff alleges infringement of United States Patents No. 7,302,708 ("the '708 Patent"), 7,685,436 ("the '436 Patent"), 8,566,612 ("the '612 Patent"), 7,916,630 ("the '630 Patent"), and 7,921,323 ("the '323 Patent"). Dkt. No. 1, Exs. 1–5; Dkt. No. 53, Ex. 1.

The '612 Patent is a continuation of the '436 Patent.

Shortly before the start of the November 17, 2023 hearing, the Court provided the parties with preliminary constructions with the aim of focusing the parties' arguments and facilitating discussion. Those preliminary constructions are noted below within the discussion for each term.

II. LEGAL PRINCIPLES

"It is a 'bedrock principle' of patent law that 'the claims of a patent define the invention to which the patentee is entitled the right to exclude.'" *Phillips*, 415 F.3d at 1312 (quoting *Innova/Pure Water Inc. v. Safari Water Filtration Sys., Inc.*, 381 F.3d 1111, 1115 (Fed. Cir. 2004)). Claim construction is clearly an issue of law for the court to decide. *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 970–71 (Fed. Cir. 1995) (en banc), *aff'd*, 517 U.S. 370 (1996). "In some cases, however, the district court will need to look beyond the patent's intrinsic evidence and to consult extrinsic evidence in order to understand, for example, the background science or the meaning of a term in the relevant art during the relevant time period." *Teva*, 135 S. Ct. at 841 (citation omitted). "In cases where those subsidiary facts are in dispute, courts will need to make subsidiary factual findings about that extrinsic evidence. These are the 'evidentiary underpinnings' of claim construction that we discussed in *Markman*, and this subsidiary factfinding must be reviewed for clear error on appeal." *Id.* (citing 517 U.S. 370).

To determine the meaning of the claims, courts start by considering the intrinsic evidence. *See Phillips*, 415 F.3d at 1313; *see also C.R. Bard, Inc. v. U.S. Surgical Corp.*, 388 F.3d 858, 861 (Fed. Cir. 2004); *Bell Atl. Network Servs., Inc. v. Covad Commc'ns Group, Inc.*, 262 F.3d 1258, 1267 (Fed. Cir. 2001). The intrinsic evidence includes the claims themselves, the specification, and the prosecution history. *See Phillips*, 415 F.3d at 1314; *C.R. Bard*, 388 F.3d at 861. Courts give claim terms their ordinary and accustomed meaning as understood by one of ordinary skill in the art at the time of the invention in the context of the entire patent. *Phillips*, 415 F.3d at 1312–13; *accord Alloc, Inc. v. Int'l Trade Comm'n*, 342 F.3d 1361, 1368 (Fed. Cir. 2003).

The claims themselves provide substantial guidance in determining the meaning of particular claim terms. *Phillips*, 415 F.3d at 1314. First, a term's context in the asserted claim can be very instructive. *Id.* Other asserted or unasserted claims can aid in determining the claim's meaning because claim terms are typically used consistently throughout the patent. *Id.* Differences among the claim terms can also assist in understanding a term's meaning. *Id.* For example, when a dependent claim adds a limitation to an independent claim, it is presumed that the independent claim does not include the limitation. *Id.* at 1314–15.

"[C]laims 'must be read in view of the specification, of which they are a part.'" *Id.* at 1315 (quoting *Markman*, 52 F.3d at 979). "[T]he specification 'is always highly relevant to the claim construction analysis. Usually, it is dispositive; it is the single best guide to the meaning of a disputed term.'" *Phillips*, 415 F.3d at 1315 (quoting *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996)); *accord Teleflex, Inc. v. Ficosa N. Am. Corp.*, 299 F.3d 1313, 1325 (Fed. Cir. 2002). This is true because a patentee may define his own terms, give a claim term a different meaning than the term would otherwise possess, or disclaim or disavow the claim scope. *Phillips*, 415 F.3d at 1316. In these situations, the inventor's lexicography governs. *Id.* The specification may also resolve the meaning of ambiguous claim terms "where the ordinary and accustomed meaning of the words used in the claims lack sufficient clarity to permit the scope of the claim to be ascertained from the words alone." *Teleflex*, 299 F.3d at 1325. But, "[a]lthough the specification may aid the court in interpreting the meaning of disputed claim language, particular embodiments and examples appearing in the specification will not generally be read into the claims." *Comark Commc'ns, Inc. v. Harris Corp.*, 156 F.3d 1182, 1187 (Fed. Cir. 1998) (quoting *Constant v. Advanced Micro-Devices, Inc.*, 848 F.2d 1560, 1571 (Fed. Cir. 1988)); *accord Phillips*, 415 F.3d at 1323.

The prosecution history is another tool to supply the proper context for claim construction because a patent applicant may also define a term in prosecuting the patent. *Home Diagnostics, Inc. v. Lifescan, Inc.*, 381 F.3d 1352, 1356 (Fed. Cir. 2004) ("As in the case of the specification, a patent applicant may define a term in prosecuting a patent."). "[T]he prosecution history (or file wrapper) limits the interpretation of claims so as to exclude any interpretation that may have been disclaimed or disavowed during prosecution in order to obtain claim allowance." *Standard Oil Co. v. Am. Cyanamid Co.*, 774 F.2d 448, 452 (Fed. Cir. 1985).

Although extrinsic evidence can be useful, it is "less significant than the intrinsic record in determining the legally operative meaning of claim language." *Phillips*, 415 F.3d at 1317 (citations and internal quotation marks omitted). Technical dictionaries and treatises may help a court understand the underlying technology and the manner in which one skilled in the art might use claim terms, but technical dictionaries and treatises may provide definitions that are too broad or may not be indicative of how the term is used in the patent. *Id.* at 1318. Similarly, expert testimony may aid a court in understanding the underlying technology and determining the particular meaning of a term in the pertinent field, but an expert's conclusory, unsupported assertions as to a term's definition are entirely unhelpful to a court. *Id.* Generally, extrinsic evidence is "less reliable than the patent and its prosecution history in determining how to read claim terms." *Id.*

The Supreme Court of the United States has "read [35 U.S.C.] § 112, ¶ 2 to require that a patent's claims, viewed in light of the specification and prosecution history, inform those skilled in the art about the scope of the invention with reasonable certainty." *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2129 (2014). "A determination of claim indefiniteness is a legal conclusion that is drawn from the court's performance of its duty as the construer of patent claims." *Datamize, LLC v. Plumtree Software, Inc.*, 417 F.3d 1342, 1347 (Fed. Cir. 2005) (citations and internal quotation marks omitted), *abrogated on other grounds by Nautilus,* 134 S. Ct. 2120. "Indefiniteness must be proven by clear and convincing evidence." *Sonix Tech. Co. v. Publ'ns Int'l, Ltd.*, 844 F.3d 1370, 1377 (Fed. Cir. 2017).

III. AGREED TERMS

The parties reached agreement on constructions as stated in their September 1, 2023 P.R. 4-3 Joint Claim Construction and Prehearing Statement (Dkt. No. 139, Ex. A) and in their November 3, 2023 P.R. 4-5(d) Joint Claim Construction Chart (Dkt. No. 149, Ex. A). Those agreements are set forth in Appendix A to the present Claim Construction Memorandum and Order.

IV. DISPUTED TERMS IN U.S. PATENT NO. 7,302,708

The '708 Patent, titled "Enforcing Computer Security Utilizing an Adaptive Lattice Mechanism," issued on November 27, 2007, and bears a filing date of March 11, 2004. The Abstract of the '708 Patent states:

> Method and apparatus for ensuring secure access to a computer system (1000). The method can begin with the step of receiving in the computer system a request from an entity (using 1002). The entity can have a predetermined access authorization level for access to a first base node (110) representing an information type (102) or a computer system function (104). The system determines if the access request completes a prohibited temporal access pattern for the entity. The system also compares a minimum access level established for the first base node to the predetermined access authorization level assigned to the entity. Thereafter, the system can grant the access request only if the minimum access level for the first base node does not exceed to the predetermined access authorization level.

1. “temporal access pattern”

<table>
<tr><th colspan="2">“temporal access pattern”
(’708 Patent, Claims 1, 9, 10, 11)</th></tr>
<tr><th>Plaintiff’s Proposed Construction</th><th>Defendants’ Proposed Construction</th></tr>
<tr><td>No construction necessary.
Plain and ordinary meaning.
Alternatively, “a sequence of operations related to time”</td><td>“a temporal relationship between two or more nodes that communicates the ordering in time of events”</td></tr>
</table>

Dkt. No. 139, Ex. B at 1; Dkt. No. 149, Ex. A at 1.

Shortly before the start of the November 17, 2023 hearing, the Court provided the parties with the following preliminary construction: “a temporal relationship between two or more accesses.”

(1) The Parties’ Positions

Plaintiff argues that “Defendants’ construction improperly seeks to import limitations from the specification in a manner that excludes a preferred embodiment.” Dkt. No. 145 at 1 (citation omitted). Plaintiff argues that there is no lexicography or disclaimer in the specification or the prosecution history that would support excluding the “single node” embodiment. *Id.* at 1–2.

Defendants respond that their proposal “comes directly from the definition the patentee provided during prosecution.” Dkt. No. 146 at 2; *see id.* at 3. Defendants also argue that “[c]ontrary to Lionra’s argument that the patent teaches an embodiment of a ‘temporal access pattern’ for ‘a single node’ rather than two or more nodes, the very paragraph Lionra cited to for its argument notes that the ‘single node’ is actually an aggregation of two base nodes, 104_1 and 104_2.” *Id.* at 3 (citing ’708 Patent at 4:3–28). Further, Defendants argue that Plaintiff’s alternative proposal of "related to time" "in effect seeks to eliminate the words 'temporal access' from the claim entirely since by definition all sequences inherently have some relation to time." *Id.* at 4. Finally, Defendants argue that "the specification also supports Defendants' proposed construction, as the completion of the temporal access pattern is discussed as the temporal relationship between two or more nodes (104_1 and 104_2) being performed in a particular temporal ordering of those access events." *Id.*

Plaintiff replies that no clear definition was provided during prosecution. Dkt. No. 148 at 1. Plaintiff also reiterates that the specification discloses a single node, and "this embodiment is consistent with Claim 1, which recites only 'a first base node' and does not require two nodes." *Id.*

At the November 17, 2023 hearing, Plaintiff agreed with the court's preliminary construction. Defendants responded by emphasizing the prosecution history and by arguing that the specification discloses nothing about an amount of time between accesses or a number of accesses within a period of time.

(2) Analysis

Claim 1 of the '708 Patent, for example, recites (emphasis added)

> 1. A method for secure access to a computer system, comprising the steps of:
>
> receiving in said computer system a request from an entity with a predetermined access level for access to a first base node representing at least one of an information type and a computer system function;
>
> determining if said access request completes a prohibited *temporal access pattern* for said entity;
>
> comparing a minimum access level established for said first base node to said predetermined access level;
>
> granting said access request only if it does not complete a prohibited *temporal access pattern* for said entity, and said minimum access level for said first base node does not exceed said predetermined access level; and
>
> denying said request if said access request completes a prohibited *temporal access pattern* for said entity.

The specification discloses:

> Referring again to FIG. 1, it can be seen that relationships can be asserted for temporal access patterns. In this figure the curved arrows labeled T1 denote a temporal ordering between the accesses defined by items 114_1 and 114_2. Thus, for item 114_2, a temporal order is asserted between items 104, [*sic*, 104_1] and 104_2, e.g. $104_1 \rightarrow 104_2$. Thus, node d(3) not only identifies an aggregation of the primitive functions denoted by 104_1 and 104_2 but also specifies that an explicit temporal ordering exists in that 104_1 is accessed before 104_2. So, for the security policy associated with item 114_2 to be activated, not only must both 104_1 and 104_2 be accessed but they must be accessed in the order indicated by the temporal relationship. In addition to specifying *a temporal order of access activities for a single node*, temporal relations may be subsumed within other nodes through aggregation. This is illustrated by item 114_1 in FIG. 1. Item 114_1 has three access items associated with the node, item 102_4, 114_2, and 104_3. As shown on the diagram, a temporal ordering has been identified that specifies $102_4 \rightarrow 114_2 \rightarrow 104_3$. However, item 114_2 is an aggregation of access operations. Thus the operations identified by item 114_2 become subsumed into the overall temporal ordering of item 114_1 and the full temporal order is $102_4 \rightarrow 104_1 \rightarrow 104_2 \rightarrow 104_3$, where item 114_2 in the original temporal order has been replaced by its constituent parts, $104_1 \rightarrow 104_2$.
>
> * * *
>
> If the request does complete a *temporal access pattern*, this means that the sequence of operations performed matches an identified pattern and is subject to the security access level specified for the that [*sic*] *temporal order*. If a temporal pattern is completed, the user's access level is compared to the access level required for the requested access action, illustrated in step 607. Note that the temporal ordering of primitive access operations mandates that the operations occur in the order specified for the security policy to be enforced. Thus, in FIG. 1, if 104_2 is accessed first followed by item 104_1, the security policy associated with node d, item 114_2, will not be activated because the temporal order was not satisfied.

'708 Patent at 4:3–28 & 5:37–48 (emphasis added); *see id.* at Fig. 1.

During prosecution, the patentee provided a "review" as follows:

> Prior to addressing the Examiner's rejections on the art, a brief review of the Applicants' invention is appropriate. The invention relates to a method and apparatus for using an adaptive lattice mechanism to enforce computer security. *See* paragraph [0023]. Generally, the method involves receiving in the computer system a request from an entity. *See* paragraphs [0009], [0033] and FIG. 6. The entity can be a user or a process and can have a predetermined access authorization level for access to a first base node representing an information type

> or a computer system function. *See* paragraph [0009]. The method also involves determining if the access request completes a prohibited temporal access pattern for the entity. *See* paragraphs [0009], [0033] and FIG. 6.
>
> In this regard, *it should be appreciated that a temporal access pattern is defined by a temporal relation between two or more nodes*. See paragraph [0028]. A temporal relation is an inter-propositional *relation that communicates the ordering in time of events*. *See* paragraph [0028] and FIG. 1. For example, a prohibited *temporal access pattern of a node A is defined by a temporal relation between an item N_1 and an item N_2, e.g., $N_1 \rightarrow N_2$.* Thus, a temporal ordering at node A exists that the item N_1 is accessed before the item N_2. So, for the security policy associated with node A to be activated, not only must the item N_1 and item N_2 be accessed but they must be accessed in the order indicated by the temporal relation.
>
> If it is determined that the access request completes a prohibited temporal access pattern for the entity, then the request is rejected. *See* paragraphs [0009], [0033] and FIG. 6. Otherwise, the method continues with a comparison of a minimum access level established for the first base node to the predetermined access authorization level assigned to the entity. *See* paragraphs [0009], [0035] and FIG. 6. If the minimum access level for the first base node does not exceed to the predetermined access authorization level, then access request is granted. *See* paragraphs [0009], [0035] and FIG. 6. However, if the minimum access level for the first base node exceeds the predetermined access authorization level assigned to the entity, then the access request is denied. *See* paragraphs [0009], [0035] and FIG. 6.

Dkt. No. 145, Ex. 1, July 12, 2007 Amendment at 7–8 (LIONRAEDTX_00000317–18) (emphasis added).

The patentee thus explained that a temporal access pattern is a temporal relation between two or more nodes. In light of the patentee's statement in that regard, the subsequent reference to "N_1" and "N_2" as "item[s]" of node A can be readily understood as referring to other nodes. Also, although the specification refers to "a temporal order of access activities for a single node" ('708 Patent at 4:16–18), and although the above-reproduced claim recites only a single ("first") node, temporal relation is necessarily with respect to two or more nodes. The patentee's definitive statement regarding "temporal access pattern" during prosecution should be given effect in the Court's construction. *See Omega Eng'g Inc. v. Raytek Corp.*, 334 F.3d 1314, 1324

(Fed. Cir. 2003) ("prosecution disclaimer promotes the public notice function of the intrinsic evidence and protects the public's reliance on definitive statements made during prosecution").

Finally, the patentee referred to "temporal relation" in terms of "ordering in time of events" (Dkt. No. 145, Ex. 1, July 12, 2007 Amendment at 8 (emphasis added)), and this, too, should be given effect in the Court's construction.

The Court therefore hereby construes **"temporal access pattern"** to mean **"a temporal relation between two or more nodes that communicates the ordering in time of events."**

2. "temporal access table"

"temporal access table" ('708 Patent, Claims 10)	
Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
No construction necessary. Plain and ordinary meaning. Alternatively, "logged access requests in a table relating to time"	"table maintaining a time-stamped history of the primitive access operations performed by a user"

Dkt. No. 139, Ex. B at 2; Dkt. No. 149, Ex. A at 3.

Shortly before the start of the November 17, 2023 hearing, the Court provided the parties with the following preliminary construction: "table maintaining a time-stamped history of accesses."

<u>(1) The Parties' Positions</u>

Plaintiff argues that "Defendants' construction improperly seeks to import limitations from an exemplary embodiment in the specification[, b]ut Defendants cannot identify any lexicography or disclaimer that warrants importing these limitations." Dkt. No. 145 at 2–3.

Defendants respond that "Defendants' proposed construction of the coined term 'temporal access table' comes directly from the specification's explanation of this coined term." Dkt. No. 146 at 5. Defendants also argue that "[h]aving no time-stamp information associated with an access request would eviscerate the disclosures in the patent." *Id.* Finally, Defendants argue: "Lionra seeks to broaden its claims well beyond what the patent discloses by using the vague and meaningless 'related to time' language, as it does for 'temporal access pattern' above. Lionra should not be permitted to eviscerate all meaning from the coined terms the patentee made up and explained in the specification." *Id.* at 6.

Plaintiff replies that "there is simply no basis to import an optional feature from one embodiment shown in Figure 4B into the claims," and "the term simply requires a 'temporal' aspect and not any precise format such as a 'time-stamped history.'" Dkt. No. 148 at 2.

<u>(2) Analysis</u>

Claim 10 of the '708 Patent recites (emphasis added)

> 10. A secure computer system comprising:
>
> a plurality of logical base nodes representing at least one of an information type and a computer system function;
>
> a plurality of higher-level nodes arranged together with said base nodes in the form of a tree hierarchy;
>
> a computer system interface capable of receiving a request from an entity with a predetermined access level for access to a first base node;
>
> a *temporal access table*;
>
> processing means programmed for comparing said access request to said *temporal access table* to determine if said access request completes a prohibited temporal access pattern for said entity, and for comparing a minimum access level established for said first base node to said predetermined access level; and
>
> wherein said processing means denies said request if said access request completes a prohibited temporal access pattern for said entity and grants said access request only if it does not complete a prohibited temporal access pattern for said entity, and said minimum access level for said first base node does not exceed said predetermined access level.

Defendants assert that "temporal access table" is a "coined" term that has no known meaning in the relevant art, and "terms coined by the inventor are best understood by reference to the specification." *Intervet Inc. v. Merial Ltd.*, 617 F.3d 1282, 1287 (Fed. Cir. 2010) (citing *Phillips*, 415 F.3d at 1315). The specification discloses:

> If the request does not complete a temporal access pattern for the particular user or the user's access level is sufficient for the temporal pattern completed, then the system continues on to step 610 and logs the request in the *Temporal Access Table* (TAT). As shown in FIG. 4B, the *Temporal Access Table* maintains a history of the primitive operations performed by a user. As a user is granted authorization to perform a primitive access operation, the operation is *time-stamped* and stored within the *TAT*. The *time stamps* are compared against the temporal patterns identified in the Temporal Order Table, FIG. 3, to check for matches. Thus, in FIG. 4B user 1 performed a dir operation at *time 102* and then requested an exec operation at *time 112*. Since 112 is after 102, this request would trigger a match in the Temporal Order Table for node d, item 114_2 in FIG. 1, and the request would be denied. However, in the case of user 3, the exec operation was performed at *time 103* followed by the dir operation at *time 111*. This pair does not match the defined temporal order and the operations are permitted.

'708 Patent at 5:51–6:2 (emphasis added).

Plaintiff argues that the disclosure of using "time stamps" is merely an example, and Plaintiff submits that the disclosed "Example 1" and "Example 2" do not refer to time stamps. '708 Patent at 7:7–12 & 7:67–8:4 (as to "Example 1" and "Example 2," disclosing "the request [being] logged in the (Temporal Access Table) as provided in step 610").

The examples cited by Plaintiff, however, refer to "comparing the *access time* to the TOT [(Temporal Order Table)]," wherein the TOT is disclosed as being "useful for capturing the relative temporal order of actions and allows relative or approximate temporal pattern matching to identify hostile actions." *Id.* at 4:31–34, 7:48–53 & 8:43–48. This reliance on "access time" reinforces the above-reproduced disclosure regarding "time stamps." *Id.* at 5:51–60. These disclosures in the specification demonstrate that time stamps are necessary in the construction of this coined term. *See Intervet*, 617 F.3d at 1287 (quoting above).

Nonetheless, no such reinforcement is provided for the disclosure regarding "primitive" access operations. Defendants' proposal of "primitive access operations" would exclude aggregations and patterns, which lacks support in the specification or the claims. Claim 10 of the '708 Patent recites "comparing said access request to said temporal access table to determine if said access request completes a prohibited temporal access pattern," and Defendants do not demonstrate that this comparison must involve only primitive access operations rather than potentially comparing an access request to aggregations or patterns maintained in a temporal access table. Defendants' reliance on the recital that a request "*completes* a prohibited temporal access pattern" is unavailing. Instead, Defendants' proposal of "primitive access operations" pertains to a specific feature of particular disclosed embodiments that should not be imported into the claims. *See Phillips*, 415 F.3d at 1323.

The Court therefore hereby construes **"temporal access table"** to mean **"table maintaining a time-stamped history of accesses by said entity."**

3. "processing means"

"processing means" ('708 Patent, Claims 10, 11)	
Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
Function 1: "comparing said access request to said temporal access table to determine if said access request completes a prohibited temporal access pattern for said entity" Structure 1: '708 patent at 1:62-64; 5:32-50; 5:51-61; 7:1-15; 7:48-60; 8:43-50; Fig. 3, 4B, 6. Function 2: "comparing a minimum access level established for said first base node to said predetermined access level" Structure 2: '708 patent at 1:64-67; 2:24-27; 3:15-42; 4:55-61; 5:37-55; 6:3- 65; 7:17-60; 8:12-9:36; Fig. 1, 4A, 5-7, 8A-8E, and 9A-9E. The elements recited in the "wherein" clause that follows are not functions, but rather further limits to the processor means element.	Function 1: comparing said access request to said temporal access table to determine if said access request completes a prohibited temporal access pattern for said entity Structure for Function 1: general purpose computer system adapted to carry out the algorithms described in '708 Patent at 1:62-64; 5:33-35, Fig. 6; 5:36-37; 5:42-47; 5:54-56, Fig. 4B; 5:56-60, Fig. 3; 5:39-42, Fig. 6; 5:46-49. Function 2: comparing a minimum access level established for said first base node to said predetermined access level Structure for Function 2: general purpose computer system adapted to carry out the algorithms described in '708 Patent at Abstract; 1:65-67; 6:2-8; Fig. 6 Function 3: denies said request if said access request completes a prohibited temporal access pattern for said entity Structure for Function 3: general purpose computer system adapted to carry out the algorithms described in '708 Patent at 1:62-64; 5:42-47, see also Fig. 1; 5:39-49, Fig. 6; 5:47-49. Function 4: grants said access request only if it does not complete a prohibited temporal access pattern for said entity, and said minimum access level for said first base node does not exceed said predetermined access level Structure for Function 4: general purpose computer system adapted to carry out the algorithms described in '708 Patent at 5:50-57; 1:67-2:3; 6:8-12, Fig. 6; 5:50-57. Function 5: denies said request if said minimum access level for said first base node exceeds said predetermined access level for said entity Structure for Function 5: general purpose computer system adapted to carry out the algorithms described in '708 Patent at 2:3-6; 6:8-12, Fig. 6. Function 6: identifies within said hierarchy any higher-level nodes that are aggregations comprising said first base node Structure for Function 6: general purpose computer system adapted to carry out the algorithms described in '708 Patent at 2:13-15; 6:42-45, Fig. 7. Function 7: identifies within said hierarchy any nodes that comprise children of any generation of said higher-level nodes that are aggregations comprising said first base node Structure for Function 7: general purpose computer system adapted to carry out the algorithms described in '708 Patent at 2:16-19; 6:48-53, Fig. 7.

Dkt. No. 139, Ex. B at 3–5.

Defendants submit: "In the interest of narrowing the disputes before the Court, Defendants agree to Lionra's proposed construction in its Opening Brief." Dkt. No. 146 at 6 (citing Dkt. 145 at 3–4).

The Court sets forth this agreement in Appendix A of this Claim Construction Order.

4. "predetermined access level"

"predetermined access level" ('708 Patent, Claims 1, 2, 9, 10, 11)	
Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
No construction necessary. Plain and ordinary meaning. Alternatively, "a security level assigned to an entity prior to an access decision"	"a security level assigned to an entity prior to an access request"

Dkt. No. 139, Ex. B at 5–6; Dkt. No. 149, Ex. A at 4.

Shortly before the start of the November 17, 2023 hearing, the Court provided the parties with the following preliminary construction: for Claims 1, 2, and 9, "a security level assigned before the 'receiving . . .' step is performed"; and for Claims 10 and 11, "a security level assigned before 'receiving a request.'"

(1) The Parties' Positions

Plaintiff argues that Defendants' proposal improperly excludes a disclosed embodiment in which a security level is assigned prior to an access *decision*. Dkt. No. 145 at 7 (discussing '708 Patent at 3:6–9 & 4:62–5:3).

Defendants respond that "[t]he plain language of the claims dictates Defendants' proposal," and "[i]n any event, Defendants' construction does not exclude any embodiment as Lionra alleges." Dkt. No. 146 at 6. Defendants argue that "Lionra cites no support for its assertion that the 'predetermined access level' in the claims can in fact *not* be 'predetermined' at all – *i.e.*, it can be determined after the access request is received, but before the access decision is made." *Id.* at 8.

Plaintiff replies that "[c]ontrary to Defendants' argument, the claim language recites 'a predetermined access level' with respect to the 'entity'—not the 'request,'" and "[t]he claim says nothing about whether the access level must be predetermined prior to an access request." Dkt. No. 148 at 2. Plaintiff also argues that "Defendants are also wrong to suggest that the 'dynamic' embodiments cannot apply to the 'predetermined access level.'" *Id.* at 3.

Defendants agreed with the Court's preliminary constructions. Plaintiff reiterated the arguments expressed in its briefing.

(2) Analysis

The claims here at issue recite "receiv[ing] in said computer system a request from an entity with a predetermined access level" ('708 Patent, Cls. 1, 9) or "receiving a request from an entity with a predetermined access level" ('708 Patent, Cl. 10). Claim 1 of the '708 Patent, for example, recites (emphasis added)

> 1. A method for secure access to a computer system, comprising the steps of:
>
> receiving in said computer system a request from an entity with a *predetermined access level* for access to a first base node representing at least one of an information type and a computer system function;
>
> determining if said access request completes a prohibited temporal access pattern for said entity;
>
> comparing a minimum access level established for said first base node to *said predetermined access level*;
>
> granting said access request only if it does not complete a prohibited temporal access pattern for said entity, and said minimum access level for said first base node does not exceed *said predetermined access level*; and
>
> denying said request if said access request completes a prohibited temporal access pattern for said entity.

Plaintiff cites disclosure in the specification that access levels can be maintained "dynamically":

> Significantly, however, the PUAT [(Process/User Access Table)] is a dynamic table in which the minimum security level required for a particular process or user to access a particular object type 102 or system function 104 can be changed depending on access history and/or identified temporal patterns. In this way, access authorities are maintained dynamically for each user allowing system objects to have multiple levels of access classification based on historical access by a particular process or user.

’708 Patent at 4:62–5:3; *see also id.* at 3:6–9 (“Access authorities are maintained dynamically for each user/process, thereby allowing system objects to have multiple levels of access classification based on historical access by each user.”).

The claim language, however, such as reproduced above, recites an “entity with a predetermined access level” and then refers back to “said predetermined access level” throughout the claim, which is contrary to Plaintiff’s suggestion that the access level could change during performance of the claimed method. Also, on its face, the word “predetermined” does not mean dynamic. Instead, a fair reading of “predetermined access level” is that this access level must be determined before the recited request is received. The other claims here at issue are similar in this regard. *See* ’708 Patent, Cls. 2, 9, 10, 11. To whatever extent this interpretation omits certain disclosed embodiments as Plaintiff argues, the claim language is clear and should be given effect. *See, e.g., SIMO Holdings Inc. v. Hong Kong uCloudlink Network Tech. Ltd.*, 983 F.3d 1367, 1378–79 (Fed. Cir. 2021) (collecting cases regarding proposition that a claim construction need not necessarily encompass all disclosed embodiments).

Finally, as Defendants argue, the above-reproduced disclosure relied upon by Plaintiff as disclosing “dynamic” access levels relates to the minimum access level required for a particular entity to access a particular node, not the predetermined access level of the entity that is requesting access. *See* ’708 Patent at 4:62–5:3; *see also id.* at 1:55–2:6 & 8:25–42.

The Court therefore hereby construes **"predetermined access level"** as set forth in the following chart:

<u>Term</u>	<u>Construction</u>
"predetermined access level" ('708 Patent, Claims 1, 2, 9)	**"a security level assigned before the 'receiving . . .' step is performed"**
"predetermined access level" ('708 Patent, Claims 10, 11)	**"a security level assigned before 'receiving a request'"**

5. "node" and "base node"

<table>
<tr><td colspan="2"><b>"node"</b>
('708 Patent, Claims 1, 2, 9, 10, 11)</td></tr>
<tr><td><b>Plaintiff's Proposed Construction</b></td><td><b>Defendants' Proposed Construction</b></td></tr>
<tr><td>No construction necessary.
Plain and ordinary meaning.
Alternatively, "a connection point in a graph."</td><td>"a connection point in a hierarchical, directed graph"</td></tr>
<tr><td colspan="2"><b>"base node"</b>
('708 Patent, Claims 1, 2, 9, 10, 11)</td></tr>
<tr><td><b>Plaintiff's Proposed Construction</b></td><td><b>Defendants' Proposed Construction</b></td></tr>
<tr><td>No construction necessary.
Plain and ordinary meaning.
Alternatively, "a node that represents an information type or computer system function."</td><td>"lowest level connection point in a hierarchical, directed graph that represents an information type or computer system function"</td></tr>
</table>

Dkt. No. 139, Ex. B at 7–8; Dkt. No. 149, Ex. A at 8–9 & 11.

Shortly before the start of the November 17, 2023 hearing, the Court provided the parties with the following preliminary constructions: "node" means "connection point in a graph"; and "base node" means "lowest-level connection point in a hierarchical graph."

(1) The Parties' Positions

Plaintiff argues that "Defendants' constructions improperly seek to import limitations from an exemplary embodiment in the specification to require that a node must be part of a graph that is 'hierarchical, directed[,' b]ut Defendants cannot identify any lexicography or disclaimer that warrants importing these limitations." Dkt. No. 145 at 8. Plaintiff also argues that "[w]hen the patentee intended to limit the claims to a hierarchical graph, the requirement was expressly recited in the claims." *Id.* (discussing '708 Patent, Cls. 1, 3, 9, 10).

As to "node," Defendants respond that "[t]he point of Defendants' construction is that 'node' is an umbrella term that includes all nodes within a given graph regardless of their levels, while 'base nodes' and 'higher-level nodes' are specific types of nodes within the hierarchy of nodes in the graph (in other words, they exist at lower or higher levels)." Dkt. No. 146 at 9. Defendants argue that "[t]he only way the specification discloses accomplishing the objective of the invention is through the use of a 'hierarchical, directed graph.'" *Id.* Defendants urge that "[t]he use of a hierarchical, directed graph is how the patent accomplishes monitoring both the access level and the temporal access pattern that is the key distinguishing feature over the prior art." *Id.*

As to "base node," Defendants respond that "[t]he specification repeatedly explains that 'base nodes' can be aggregated to 'higher-level nodes,'" and "[t]hus, 'base nodes' are the lowest-level nodes that can be aggregated into 'higher-level nodes.'" Dkt. No. 146 at 11 (citing '708 Patent at 2:11–12, 2:19–23, 2:67–3:3 & 3:48–52). Defendants also argue that "Lionra's proposal simply restates the claim language," and that "claim language says what a base node 'represents,' not what it actually *is*." *Id.* Further, Defendants argue that "Lionra's proposal renders superfluous the term 'base,' redefining 'base node' as simply a 'node.'" *Id.* at 12.

Plaintiff replies that “both the claims and specification confirm that the term ‘base node’ (for example in claim 1) does not require the hierarchical structure argued by Defendants.” Dkt. No. 148 at 3.

At the November 17, 2023 hearing, Plaintiff argued that the term “base node” does not imply a hierarchical graph because “base” nodes could be, for example, edges of a linear graph. Defendants argued that the graph must be “directed” because the claimed inventions require ordering, as shown, for example, by the arrows in Figure 1 of the ’708 Patent.

(2) Analysis

Claim 1 of the ’708 Patent, for example, recites (emphasis added):

> 1. A method for secure access to a computer system, comprising the steps of:
>
> receiving in said computer system a request from an entity with a predetermined access level for access to a first *base node representing at least one of an information type and a computer system function*;
>
> determining if said access request completes a prohibited temporal access pattern for said entity;
>
> comparing a minimum access level established for said first *base node* to said predetermined access level;
>
> granting said access request only if it does not complete a prohibited temporal access pattern for said entity, and said minimum access level for said first *base node* does not exceed said predetermined access level; and
>
> denying said request if said access request completes a prohibited temporal access pattern for said entity.

As for Defendants’ proposal of requiring a “directed” graph, the specification discloses:

> The invention concerns a method and system for using an adaptive lattice mechanism to enforce computer security. Data and function access security levels form an initial basis for controlling access. These security access primitives *can be* organized within a partially ordered set (POSET) so as to define a *hierarchical, directed graph*. The security access primitives can form *base nodes in the hierarchical, directed graph*. Higher level nodes within the graph represent information aggregation sets and/or temporal patterns of access. Each of the nodes within the graph can have an associated security level representing the mandatory security level for the particular aggregation or pattern. Access authorities are maintained dynamically for each user/process, thereby allowing system objects to have multiple levels of access classification based on historical access by each user.

> * * *
>
> As illustrated in FIG. 1, higher-level nodes 112 can include aggregations of base nodes 110, as well as higher order aggregations, i.e. aggregations of previously constructed aggregations.
>
> According to one embodiment of the invention, the *hierarchical directed* graph of FIG. 1 can be implemented by organizing the object types 102_1–102_4 and system functions 104_1–104_3 within a partially ordered set (POSET). A POSET defines relationships that exist between pairs of elements, e.g. x→R→y within a set of elements. Within the set of elements, there exists pairs of elements, e.g. m and n, for which no relation R exists. Thus, the set is partially ordered. Consequently, POSETs may have multiple root and leaf nodes in contrast to a tree structure which has a single root node and multiple leaf nodes.

’708 Patent at 2:62–3:9 & 3:53–63 (emphasis added); *see id.* at 2:11–12, 2:19–23 & 3:48–52.

This disclosure of how security access primitives “*can be* organized” (*id.* at 2:62–3:9 (emphasis added)) is not limiting but rather relates to specific features of particular disclosed embodiments that should not be imported into the claims. *See Phillips*, 415 F.3d at 1323.

Defendants cite the following disclosure as support for requiring “node” and “base node” to refer to a “directed” graph:

> In [Figure 1] the curved arrows labeled T1 denote a temporal ordering between the accesses defined by items 114_1 and 114_2. Thus, for item 114_2, a temporal order is asserted between items 104, [*sic*, 104_1] and 104_2, e.g. $104_1 \rightarrow 104_2$. Thus, node d(3) not only identifies an aggregation of the primitive functions denoted by 104_1 and 104_2 but also specifies that an explicit temporal ordering exists in that 104_1 is accessed before 104_2. So, for the security policy associated with item 114_2 to be activated, not only must both 104_1 and 104_2 be accessed but they must be accessed in the order indicated by the temporal relationship. In addition to specifying a temporal order of access activities for a single node, temporal relations may be subsumed within other nodes through aggregation. This is illustrated by item 114_1 in FIG. 1. Item 114_1 has three access items associated with the node, item 102_4, 114_2, and 104_3.

’708 Patent at 4:4–20.

Particularly when considering that the claims separately recite "a prohibited temporal access pattern," this disclosure cited by Defendants regarding a particular disclosed embodiment does not warrant introducing a "directed" graph requirement into the claims.

As for whether a "node" or a "base node" must be part of a "graph," construction is appropriate in this regard because the parties agree that a "node" is a "connection point" in a "graph." Because the word "node" can have various different meanings depending on the technical context (as wide-ranging as, for example, telecommunications or human anatomy), "some construction of the disputed claim language will assist the jury to understand the claims." *TQP Dev., LLC v. Merrill Lynch & Co.*, No. 2:08-CV-471-WCB, 2012 WL 1940849, at *2 (E.D. Tex. May 29, 2012) (Bryson, J., sitting by designation).

As for Defendants' proposal of a "hierarchical" graph, some of the claims recite "base nodes" as well as "higher-level nodes" (which is a separately disputed term addressed below), and all of the claims recite "base" nodes rather than merely "nodes," which implies that there can be multiple levels of nodes. Read in light of the above-cited disclosures in the specification, a fair reading of the claims is that a "base node" is implicitly part of a "hierarchy." Plaintiff's argument at the November 17, 2023 hearing that "base" nodes could be the "edges" of a "linear" graph lacks support in any intrinsic or extrinsic evidence.

Plaintiff also points to dependent Claim 3 of the '708 Patent, which recites "a tree hierarchy having a plurality of leaf nodes and higher-level nodes." This dependent claim adds several other limitations, not just a hierarchy. Claim 3 is thus *not* inconsistent with finding that a "base node" as necessarily being part of a hierarchy. Plaintiff's reliance on the recitals of a "tree hierarchy" in Claims 9 and 10 is similarly unavailing. Nonetheless, a hierarchical graph need not necessarily be a "tree hierarchy," which is recited in only some of the claims.

Finally, Plaintiff argues that Defendants' proposal of construing "base node" as a "lowest level connection point" should be rejected because surrounding claim language already recites a "base node representing at least one of an information type and a computer system function." The word "base," however, is presumed to have meaning because "[c]laims must be 'interpreted with an eye toward giving effect to all terms in the claim.'" *Becton, Dickinson & Co. v. Tyco Healthcare Grp., LP*, 616 F.3d 1249, 1257 (Fed. Cir. 2010) (quoting *Bicon, Inc. v. Straumann Co.*, 441 F.3d 945, 950 (Fed. Cir. 2006)). The contrast between "base nodes" and "higher-level nodes" throughout the claims, as well as the above-cited disclosures in the specification, demonstrates that "base" refers to the lowest level.

The Court therefore hereby construes these disputed terms as set forth in the following chart:

Term	Construction
"node"	**"connection point in a graph"**
"base node"	**"lowest-level connection point in a hierarchical graph"**

6. "arranged together with said base nodes in the form of a tree hierarchy"

"arranged together with said base nodes in the form of a tree hierarchy" ('708 Patent, Claim 9)	
Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
Preamble for claim 9 is not limiting. No construction necessary.	Preamble is limiting.

Dkt. No. 139, Ex. B at 9.

Plaintiff submits: "In an effort to limit the number of disputes for the Court, Lionra agrees that the preamble language 'arranged together with said base nodes in the form of a tree hierarchy' is limiting." Dkt. No. 145 at 9.

The Court sets forth this agreement in Appendix A of this Claim Construction Order.

7. "higher-level nodes"

"higher-level nodes" ('708 Patent, Claims 9, 10)	
Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
No construction necessary. Plain and ordinary meaning. Alternatively, "nodes at a level in the tree hierarchy higher than the root (base) node."	"nodes within a hierarchical, directed graph that represent aggregations of base nodes, and/or temporal patterns of access"

Dkt. No. 139, Ex. B at 6–7; Dkt. No. 149, Ex. A at 7.

Shortly before the start of the November 17, 2023 hearing, the Court provided the parties with the following preliminary construction: "aggregations of other nodes or of temporal patterns of access or of both."

<u>(1) The Parties' Positions</u>

Plaintiff argues that "Defendants' construction improperly seeks to import limitations from an exemplary embodiment in the specification that a 'higher-level node' must 'represent aggregations of base nodes, and/or temporal patterns of access[, b]ut Defendants cannot identify any lexicography or disclaimer that warrants importing these limitations." Dkt. No. 145 at 10. "To the contrary," Plaintiff argues, "the specification makes clear that higher-level nodes are not necessarily required to be aggregations of base nodes . . . ." *Id.* (citing '708 Patent at 3:47–48 & 3:53–54). Further, Plaintiff argues that "the patentee expressly included the 'aggregation' requirement when it intended to include this requirement in the claims." *Id.* at 10–11.

Defendants respond that "Lionra's proposal fails to acknowledge the very premise of the invention: the ability to evaluate temporal patterns of access." Dkt. No. 146 at 12.

Plaintiff replies that "Defendants improperly seek to import further limitations from an exemplary embodiment in the specification without identifying any lexicography or disclaimer that supports their construction." Dkt. No. 148 at 4.

At the November 17, 2023 hearing, Defendants were amenable to the Court's preliminary construction. Plaintiff responded that a higher-level node need not be an aggregation of nodes because a temporal access pattern does not require multiple nodes. Plaintiff also argued that a higher-level node need not be an *aggregation* of temporal patterns.

(2) Analysis

Claims 9 and 10 of the '708 Patent recite (emphasis added):

> 9. A method for restricting access to a computer system having a plurality of logical base nodes representing at least one of an information type and a computer system function, and a plurality of *higher-level nodes* arranged together with said base nodes in the form of a tree hierarchy, comprising the steps of:
>
> receiving in said computer system a request from an entity with a predetermined access level for access to a first base node;
>
> determining if said access request completes a prohibited temporal access pattern for said entity;
>
> comparing a minimum access level established for said first base node to said predetermined access level;
>
> granting said access request only if it does not complete a prohibited temporal access pattern for said entity, and said minimum access level for said first base node does not exceed said predetermined access level; and
>
> denying said request if said access request completes a prohibited temporal access pattern for said entity.
>
> 10. A secure computer system comprising:
>
> a plurality of logical base nodes representing at least one of an information type and a computer system function;
>
> a plurality of *higher-level nodes* arranged together with said base nodes in the form of a tree hierarchy;
>
> a computer system interface capable of receiving a request from an entity with a predetermined access level for access to a first base node;
>
> a temporal access table;

> processing means programmed for comparing said access request to said temporal access table to determine if said access request completes a prohibited temporal access pattern for said entity, and for comparing a minimum access level established for said first base node to said predetermined access level; and
>
> wherein said processing means denies said request if said access request completes a prohibited temporal access pattern for said entity and grants said access request only if it does not complete a prohibited temporal access pattern for said entity, and said minimum access level for said first base node does not exceed said predetermined access level.

The specification discloses:

> *Higher level nodes within the graph represent information aggregation sets and/or temporal patterns of access.*
>
> * * *
>
> The various object types 102_1–102_4 and system functions 104_1–104_3 can be represented in a hierarchical tree graph as shown in FIG. 1. According to one aspect of the invention, the various object types and system functions can be defined as a plurality of leaf or base nodes 110 in the hierarchical tree 100. Further, *higher-level nodes 112 can be constructed to represent aggregations of base nodes 110*. As illustrated in FIG. 1, *higher-level nodes 112 can include aggregations of base nodes 110*, as well as higher order aggregations, i.e. aggregations of previously constructed aggregations.
>
> According to one embodiment of the invention, the hierarchical directed graph of FIG. 1 can be implemented by organizing the object types 102_1–102_4 and system functions 104_1–104_3 within a partially ordered set (POSET).

’708 Patent at 3:2–3 & 3:43–56 (emphasis added); *see id.* at Fig. 1.

The specification thus refers to “higher-level nodes” in terms of “information aggregation sets and/or temporal patterns of access” and in terms of “aggregations of base nodes.”

As for whether the construction should refer to an aggregation of “base” nodes, Claim 12 depends from Claim 10 and recites:

> 12. The secure computer system according to claim 10 wherein said higher-level nodes are aggregations of said base nodes.

This dependent claim weighs at least somewhat against limiting aggregations to being of base nodes. *See Phillips*, 415 F.3d at 1315 (“the presence of a dependent claim that adds a particular limitation gives rise to a presumption that the limitation in question is not present in the independent claim") (citation omitted).

Thus, based on the above-discussed disclosures in the specification that explain a "higher-level node" in relation to other nodes, and further considering the Court's construction of "temporal access pattern" (which is a disputed term addressed above) as involving two or more nodes, the Court's construction should refer to a temporal access pattern, or an aggregation of other nodes, or a combination of a temporal access pattern and at least one other node.

The Court therefore hereby construes **"higher-level nodes"** to mean **"a temporal access pattern, or an aggregation of other nodes, or a combination of a temporal access pattern and one or more other nodes."**

V. DISPUTED TERMS IN U.S. PATENTS NO. 7,685,436 AND 8,566,612

The '436 Patent, titled "System and Method for a Secure I/O Interface," issued on March 23, 2010, and bears an earliest priority date of October 2, 2003. The Abstract of the '436 Patent states:

> A security processor performs all or substantially all security and network processing to provide a secure I/O interface system to protect computing hardware from unauthorized access or attack. The security processor sends and receives all incoming and outgoing data packets for a host device and includes a packet engine, coupled to a local data bus, to process the incoming and outgoing packets. The processor further comprises a cryptographic core coupled to the packet engine to provide encryption and decryption processing for packets processed by the packet engine. The packet engine also handles classification processing for the incoming and outgoing packets. A modulo engine may be coupled to the local data bus.

8. “substantially all of the incoming and outgoing packets to the security processor transit one of the plurality of packet engines”

<table>
<tr><td colspan="2"><b>“substantially all of the incoming and outgoing packets to the security processor transit one of the plurality of packet engines”</b>
(’436 Patent, Claims 1, 13;
’612 Patent, Claims 1, 13)</td></tr>
<tr><td><b>Plaintiff’s Proposed Construction</b></td><td><b>Defendants’ Proposed Construction</b></td></tr>
<tr><td>No construction necessary.
Plain and ordinary meaning.
Not indefinite.</td><td>Indefinite</td></tr>
</table>

Dkt. No. 139, Ex. B at 10; Dkt. No. 149, Ex. A at 14.

Shortly before the start of the November 17, 2023 hearing, the Court provided the parties with the following preliminary construction: “Plain meaning.”

(1) The Parties’ Positions

Plaintiff argues that “[t]he meaning of the disputed term is readily understood by a POSITA based on the intrinsic evidence.” Dkt. No. 145 at 12 (citations omitted). “For example,” Plaintiff argues, “the specification explains that protection against unauthorized access may be achieved by ‘routing all or substantially all I/O to and from host processor 130 and/or internal network 116 through security processing system 102.’” *Id.* (quoting ’436 Patent at 4:29–47). Plaintiff also argues that “Defendants’ criticisms are purely conjecture and rely solely on attorney argument.” *Id.* at 13. Further, Plaintiff submits that “‘[a]bsolute precision’ in claim language is ‘unattainable’ and that “the Federal Circuit has faulted courts for attempting to introduce ‘numerical’ limitations on terms reciting ‘substantially.’” *Id.* at 14 (citations omitted). Finally, Plaintiff argues that even if “substantially” were deemed to be a term of degree, “the patents provide a standard by which the term is measured—i.e., less than ‘all’ packets—and the claim is definite," and "Defendant Cisco had no issue applying the term to the alleged prior art [in IPR petitions], which underscores that the term can be understood with reasonable certainty." *Id.* at 14–15 (citation omitted).

Defendants respond that "[a] person of ordinary skill in the art would not be able to discern with reasonable certainty how many packets have to go through the packet engines in order to meet the threshold of 'substantially all' as required by the claim," and "[t]he specification fails to shed any light on the objective boundaries of this term." Dkt. No. 146 at 15. Defendants also argue that, during prosecution, "despite the inclusion of this term being the lynchpin to allowing the claims, the applicant provided no explanation whatsoever on what the term actually means." *Id.* at 16. Finally, as to the IPR proceedings, Defendants note that IPR petitioners are not permitted to assert indefiniteness. *Id.* at 18.

Plaintiff replies that "the fact that 'substantially' modifies 'all' to account for dropped packets, for example, does not render Claims 1 and 13 indefinite." Dkt. No. 148 at 4–5 (footnote omitted). Plaintiff argues that "Defendants' argument that 'only 1% of all the packets would also meet the claim limitation because it would be fewer than all' (Resp. at 16) is unpersuasive because it completely ignores the plain and ordinary meaning of the word 'substantially.'" *Id.* at 5 n.5.

(2) Analysis

As a threshold matter, the IPR proceedings cited by Plaintiff (*see* Dkt. No. 145 at 15) are unpersuasive because an IPR petition cannot assert indefiniteness. *See* 35 U.S.C. § 311(b); *see also Cuozzo Speed Tech., LLC v. Lee*, 136 S. Ct. 2131, 2141–42 (2016).

Turning to the claim language, Claim 1 of the '436 Patent, for example, recites (emphasis added):

> 1. A security processor to process incoming packets and outgoing packets, the security processor comprising:
>
> a switching system to send the outgoing packets and receive the incoming packets;
>
> a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system, wherein the packet engine is one of a plurality of packet engines and *substantially all of the incoming packets and outgoing packets to the security processor transit one of the plurality of packet engines*, and wherein the incoming packets and outgoing packets are provided with a tag upon ingress to one of the plurality of packet engines and the tag determines an egress path within the security processor upon exit from a corresponding cryptographic core;
>
> a cryptographic core, coupled to the packet engine and receiving the incoming packets from the switching system via the packet engine and communicating the outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core;
>
> a signature database; and
>
> an intrusion detection system coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database.

"The claims, when read in light of the specification and the prosecution history, must provide objective boundaries for those of skill in the art." *Interval Licensing LLC v. AOL, Inc.*, 766 F.3d 1364, 1371 (Fed. Cir. 2014); *see id.* at 1370–71 (requiring "some standard for measuring the scope of the phrase") (quoting *Datamize, LLC v. Plumtree Software, Inc.*, 417 F.3d 1342, 1351 (Fed. Cir. 2005)).

The Federal Circuit has "repeatedly confirmed that relative terms such as 'substantially' do not render patent claims so unclear as to prevent a person of skill in the art from ascertaining the scope of the claim." *Deere & Co. v. Bush Hog, LLC*, 703 F.3d 1349, 1359 (Fed. Cir. 2012); *see Enzo Biochem, Inc. v. Applera Corp.*, 599 F.3d 1325, 1335 (Fed. Cir. 2010) ("precise numerical measurement" not required) (citations omitted); *see also Liquid Dynamics Corp. v. Vaughan Co.*, 355 F.3d 1361, 1368 (Fed. Cir. 2004) ("term 'substantial' is a meaningful modifier implying 'approximate,' rather than 'perfect'") (citation omitted); *Anchor Wall Sys. Inc. v. Rockwood Retaining Walls, Inc.*, 340 F.3d 1298, 1310–11 (Fed. Cir. 2003) ("words of approximation, such as 'generally' and 'substantially,' are descriptive terms . . . 'to avoid a strict numerical boundary'") (citation omitted).

The specification discloses:

> Security processing system 102 may be coupled to internal network 116 by I/O interface 114 and to external network 120 by I/O interface 118. Interfaces 114 and 118 may perform physical (PHY) layer processing to convert a digital bit stream to or from an analog or photonic signal for transmission over a physical medium such as, for example, copper wire pairs, co-axial cable, fiber or air. Interfaces 114 and 118 are, for example, streaming data interfaces such as a Packet-Over-SONET Physical-Layer Three (POS/PHY3) type streaming interface, although 10/100 megabit (Mb) Ethernet, 1 Gigabit (Gb) Ethernet, UTOPIA, LX SPI-4 and other interface types may be suitable. By routing *all or substantially all* I/O to and from host processor 130 and/or internal network 116 through security processing system 102, host processor 130 and internal network 116 are *substantially protected* against unauthorized access or other security breaches, protecting the security information integrity, and providing processing and storage efficiency from information consolidation.

'436 Patent at 4:29–47 (emphasis added).

The specification also discloses that packet engines may perform various operations including potentially "dropping the packet":

> In one embodiment, all incoming packets to security processor 104 may be initially processed by one of packet engines 228. Each packet engine 228 may classify the packet based upon a lookup table result and then may apply a variety of operations including, for example, forwarding with necessary transform parameters to cryptographic core 232, or forwarding to control processor 212 for application level processing. Such operations may further include overwriting portions of the packet with new data such as, for example, the media access control (MAC) header for forwarding and the IP header for NAT, and may also include *dropping the packet*, or passing the packet through security processor 104 to an egress interface, such as, for example, streaming interface 200, unchanged.

Id. at 11:9–22 (emphasis added).

At the November 17, 2023 hearing, Defendants argued that the above-reproduced disclosure in the specification regarding packets potentially being dropped *by* the packet engines is irrelevant because the "substantially all" limitation relates to packets *arriving at* the packet engines. That is, Defendants argued that the reference in this disputed term to packets that "transit one of the plurality of packet engines" refers to packets *arriving at* the packet engines rather than to packets *passing through* the packet engines. Defendants cited the patentee's usage of "transit through" and "transit to" in the specification. *Id.* at 20:30 & 20:54.

The claims, however, recite "transit," not "transit to." The Court rejects Defendants' interpretation that the "transit" limitation refers to packets merely arriving at the packet engines. The claims require that the packet engines *operate on* "the incoming packets," meaning all of them, and the "substantially all . . ." limitation expresses that not every packet *passes through* the packet engines.

The patents provide no numerical lower boundary for "substantially all," but the claim scope is reasonably clear in light of the above-cited authorities and in light of the context provided by the specification regarding "dropping" some packets. The opinions of Plaintiff's expert are further persuasive in this regard. *See* Dkt. No. 145, Ex. 3, Sept. 1, 2023 Smith Decl. at ¶ 24 ("although packets may be passed as input into at least one of the packet engines, not all of the packets will be output and, consequently, not transit from the packet engine to the security processor"); *see also id.* at ¶¶ 21–24.

The *Fiber* and *Geodynamics* cases cited by Defendants are distinguishable. In *Fiber*, the court found the term "substantially a complete set" to be indefinite, noting: "There is nothing in the specification that clarifies what portion of a 'complete set' would be a 'substantially complete set.' It might be a majority or, as plaintiff originally urged, 'at least one.'" *Fiber LLC* *v. Ciena Corp.*, No. 13-cv-00840-PAB-KLM, 2017 WL 3896443, at *13 (D. Colo. Sept. 6, 2017). In the present case, the specification discloses that substantially all packets are routed through a security processing system, and thus "host processor 130 and internal network 116 are *substantially* protected against unauthorized access or other security breaches." '436 Patent at 4:29–47 (emphasis added). The word "substantially" is thus used to allow for being less than "perfect." *Liquid Dynamics*, 355 F.3d at 1368.

In *Geodynamics*, the evidence included a wide range of possible values that "would appear to stretch well below and beyond 'substantially equal.'" *Geodynamics, Inc. v. Dynaeregetics US, Inc.*, No. 2:15-cv-1546-RSP, 2016 WL 6217181, at *15–*16 (E.D. Tex. Oct. 25, 2016) (relevant values ranged from 35% to 235%). No such evidence exists in the present case. Rather, the word "substantially" is used to allow for less than "perfect." *Liquid Dynamics*, 355 F.3d at 1368.

Finally, the prosecution history cited by Defendants, in which the patentee amended independent claims to include limitations from dependent claims that the examiner had found allowable, does not demonstrate any lack of reasonable certainty as to "substantially all of the incoming and outgoing packets to the security processor transit one of the plurality of packet engines." *See* Dkt. No. 146, Ex. A, Amendment After Final at pp. 2, 4 & 7 (pp. 264, 266 & 269 of 321 of Ex. A).

In sum, Defendants have not met their burden to show indefiniteness. Defendants present no alternative proposed construction, and no further construction is necessary.

The Court therefore hereby construes **"substantially all of the incoming and outgoing packets to the security processor transit one of the plurality of packet engines"** to have its **plain meaning**.

9. “packet engine”

<table>
<tr><th colspan="2"><b>“packet engine”</b>
(’436 Patent, Claims 1, 2, 11, 13;
’612 Patent, Claims 1, 13)</th></tr>
<tr><th>Plaintiff’s Proposed Construction</th><th>Defendants’ Proposed Construction</th></tr>
<tr><td>No construction necessary.
Plain and ordinary meaning.
Alternatively, “hardware or microprocessor customized for packet operations”</td><td>“hardware customized for packet operations, including at least packet processing and classification”[1]</td></tr>
</table>

Dkt. No. 139, Ex. B at 11; Dkt. No. 149, Ex. A at 16.

Shortly before the start of the November 17, 2023 hearing, the Court provided the parties with the following preliminary construction: “hardware, software, or a combination thereof, that is configured to perform packet operations.”

<u>(1) The Parties’ Positions</u>

Plaintiff argues that “there is no lexicography or disavowal by the patentee that supports Defendants’ limiting construction.” Dkt. No. 145 at 15 (citation omitted). Plaintiff urges that “[t]he ’436 and ’612 Patent specifications make clear that the recited ‘packet engine’ is not limited to ‘hardware’ and expressly contemplate that the ‘packet engine’ may comprise hardware and/or software (or combinations thereto), such as a ‘microprocessor.’” *Id.* (citing ’436 Patent at 5:36–49, 6:38–45, 9:60–10:6, 10:55–11:8 & 12:60–13:30). Plaintiff also argues that these patents “use the term ‘packet engine’ and ‘microprocessor’ interchangeably,” and “[a]s such, the ’436 and ’612 Patents expressly contemplate that the ‘packet engine’ is not limited to hardware and may comprise a microprocessor.” *Id.* at 16.

[1] Defendants previously proposed: “hardware customized for packet processing and classification.” Dkt. No. 139, Ex. B at 11.

Defendants respond that "Lionra offers no support, from the specification or otherwise, for the notion that a 'packet engine' or 'microprocessor' can be software alone, or even software in combination with hardware." Dkt. No. 146 at 19. Defendants also argue that "[t]he claims are system claims directed to a security processor that includes specific hardware components through which packets transit," and "[t]his plain language of the claims dictates the physical arrangement of hardware components; a concept that would not apply to software." *Id.* at 20.

Plaintiff replies that "[a]ny construction of 'packet engine' should include a 'microprocessor' because the '436 and '612 Patents use the terms interchangeably, and a microprocessor is not limited to 'hardware,'" and "a microprocessor, by definition, utilizes software." Dkt. No. 148 at 6.

At the November 17, 2023 hearing, Plaintiff agreed with the Court's preliminary construction. Defendants argued that software, by itself, would be insufficient.

(2) Analysis

Claim 1 of the '436 Patent, for example, recites (emphasis added):

> 1. A security processor to process incoming packets and outgoing packets, the security processor comprising:
>
> a switching system to send the outgoing packets and receive the incoming packets;
>
> a *packet engine*, coupled to the switching system, to handle classification processing for the incoming packets received by the *packet engine* from the switching system and the outgoing packets sent by the *packet engine* to the switching system, wherein the *packet engine* is one of a plurality of *packet engine*s and substantially all of the incoming packets and outgoing packets to the security processor transit one of the plurality of *packet engines*, and wherein the incoming packets and outgoing packets are provided with a tag upon ingress to one of the plurality of *packet engines* and the tag determines an egress path within the security processor upon exit from a corresponding cryptographic core;
>
> a cryptographic core, coupled to the *packet engine* and receiving the incoming packets from the switching system via the *packet engine* and communicating the outgoing packets to the switching system via the *packet engine*, to provide encryption and decryption processing for packets received

> from and sent to the *packet engine*, wherein the *packet engine* is interposed between the switching system and the cryptographic core;
>
> a signature database; and
>
> an intrusion detection system coupled between the cryptographic core and the *packet engine* and responsive to at least one packet matching a signature stored in the signature database.

The parties agree that the preambles of Claim 1 of the '436 Patent and Claim 1 of the '612 Patent are limiting. The disputed term here at issue, "packet engine," is thus recited as being part of the "security processor" that is recited in the preambles. Because "processor" can be readily understood as something that implements programming, the "packet engine" could be implemented as hardware or as a combination of hardware and software.

The recitals that the packet engine is "coupled to the switching system" and "interposed between the switching system and the cryptographic core" do not warrant limiting "packet engine" to being distinct hardware because processing is inherently implemented on some type of hardware and because "coupled" and "interposed" do not necessarily refer to physical relationships but rather can be understood as also encompassing processing relationships and communication relationships. Defendants' reliance on the recital that packets "transit" a packet engine is likewise unavailing.

Defendants' proposal to limit "packet engine" to distinct, separate hardware is therefore hereby expressly rejected. The specification reinforces this understanding by disclosing that packet engines can be, for example, customized microprocessors:

> Packet engines 228 may each be interposed between a cryptographic core 232 and the switching system 208 as shown in FIG. 2. Packet engines 228 may each comprise microprocessors customized for packet operations such as, for example, packet processing and classification.

'436 Patent at 9:60–64; *see id.* at 6:43–45 ("Security processor 104 is preferably, though not necessarily, formed on a single chip."); *see also id.* at 5:36–49 ("Security processing system 102 may be implemented, for example, as a stand-alone system box or as a card such as, for example, a NIC, that connects to a slot in the motherboard of a host system.").

> In parallel operation, the individual *packet engines* 228 may each independently process discrete packets and forward the packets to other devices, such as cryptographic processing cores or switches. Two or more *microprocessors* could, for example, be serialized to perform discrete functional tasks as the packet transits from one functional block to another. *Packet engines* 228, in conjunction with cryptographic cores 232 and under the common control of control processor 212, may perform, for example, firewall lookup and statistics, IPSec and secure sockets layer (SSL) processing, quality of service (QoS), traffic management, and public key processing.

Id. at 10:55–11:8. The specification thus reinforces that "packet engines" can be implemented on a processor rather than being special-purpose hardware. Likewise, dependent Claim 4 recites that "the packet engine, the cryptographic core, and the modulo engine are formed on a single chip," thus further reinforcing that a "packet engine" need not be a separate piece of hardware.

Defendants also cite disclosure that another component (the "network intrusion detection system (NIDS)") has "taps" that may "couple" to a packet engine (*id.* at 18:41–43), but the specification contains no disclosure that describes a "tap" as necessarily being a physical component, and in any event this disclosure of "taps" is part of a disclosed "example." *Id.* at 18:35–43. Defendants likewise submit no evidence to support finding that "taps" would be understood by a person of ordinary skill in the art as being limited to physical structures. Particularly when considering the other above-discussed intrinsic evidence, the disclosure of "taps" does not support a narrow reading of "packet engine."

Further, the prosecution history cited by Defendants, in which the patentee added the word "interposed," contains no definition or disclaimer or explanation that would warrant limiting "packet engine" to being distinct hardware or to otherwise necessarily being physically distinct. *See* Dkt. No. 146, Ex. A, Aug. 11, 2008 Office Action Response at pp. 2, 4 & 7 (pp. 193, 195 & 198 of 321 of Ex. A); *id.*, Apr. 27, 2009 Office Action Response at pp. 2 & 9 (pp. 225 & 232 of 321 of Ex. A).

Finally, Defendants propose that a "packet engine" must be for "at least packet processing and classification," but surrounding claim language in Claims 1 and 13 of the '436 Patent and Claims 1 and 13 of the '612 Patent already recites "a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system." Defendants' proposal is therefore redundant and would tend to confuse rather than clarify the scope of the claims.

The Court thus rejects Defendants' proposed construction, but whereas Plaintiff proposes that no construction is necessary, "some construction of the disputed claim language will assist the jury to understand the claims." *TQP*, 2012 WL 1940849, at *2.

The Court therefore hereby construes **"packet engine"** to mean **"hardware, or a combination of hardware and software, that is configured to perform packet operations."**

10. "cryptographic core"

<table>
<tr><td colspan="2"><b>"cryptographic core"</b>
('436 Patent, Claims 1, 13;
'612 Patent, Claims 1, 13)</td></tr>
<tr><td><b>Plaintiff's Proposed Construction</b></td><td><b>Defendants' Proposed Construction</b></td></tr>
<tr><td>No construction necessary.
Plain and ordinary meaning.
Alternatively, "hardware or microprocessor customized for security processing"</td><td>"hardware customized for security processing, including at least encryption and decryption"[2]</td></tr>
</table>

[2] Defendants previously proposed: "hardware customized for security processing in the form of encryption and decryption." Dkt. No. 139, Ex. B at 14.

Dkt. No. 139, Ex. B at 14; Dkt. No. 149, Ex. A at 21–22.

Shortly before the start of the November 17, 2023 hearing, the Court provided the parties with the following preliminary construction: "hardware, software, or a combination thereof, that is configured to perform cryptographic processing."

(1) The Parties' Positions

Plaintiff argues that "[b]ecause the '436 and '612 Patents include examples of cryptographic cores that utilize software, Defendants' construction limiting the 'cryptographic core' to only hardware is improper." Dkt. No. 145 at 18. Plaintiff also argues that "the '436 and '612 Patents do not limit the functionality of the 'cryptographic core' to only performing 'security processing in the form of encryption and decryption.'" *Id.* at 19.

Defendants respond that the specification discloses the cryptographic core as being hardware and as performing at least encryption and decryption. Dkt. No. 146 at 22. Defendants also argue that "the claims describe a security processor architecture having distinct hardware components through which packets transit." *Id.* Defendants also argue that, during prosecution, "the Applicants distinguished prior art that did not include the same physical arrangement of hardware, e.g., a packet engine 'interposed between' the switching system and cryptographic core, through which packets transit." *Id.* at 23.

Plaintiff replies that "[t]he patents indisputably cover cryptographic cores with software implementations." Dkt. No. 148 at 8. Plaintiff also argues that "[t]he claims already delineate the requirements of the 'cryptographic core,' and Defendants do not point to any lexicography or disclaimer that warrant re-drafting the term." *Id.*

At the November 17, 2023 hearing, Plaintiff agreed with the Court's preliminary construction. Defendants argued that software, by itself, would be insufficient.

(2) Analysis

Claim 1 of the '436 Patent, for example, recites (emphasis added):

> 1. A security processor to process incoming packets and outgoing packets, the security processor comprising:
>
> a switching system to send the outgoing packets and receive the incoming packets;
>
> a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system, wherein the packet engine is one of a plurality of packet engines and substantially all of the incoming packets and outgoing packets to the security processor transit one of the plurality of packet engines, and wherein the incoming packets and outgoing packets are provided with a tag upon ingress to one of the plurality of packet engines and the tag determines an egress path within the security processor upon exit from a corresponding *cryptographic core*;
>
> a *cryptographic core*, coupled to the packet engine and receiving the incoming packets from the switching system via the packet engine and communicating the outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the *cryptographic core*;
>
> a signature database; and
>
> an intrusion detection system coupled between the *cryptographic core* and the packet engine and responsive to at least one packet matching a signature stored in the signature database.

The dispute as to "cryptographic core" is similar to the dispute regarding "packet engine," which is addressed above, and for essentially the same reasons the Court reaches the same conclusion. Additional evidence cited by Defendants as to "cryptographic core" does not compel otherwise. Disclosures regarding forwarding packets to "other devices," for example, does not warrant limiting the term "cryptographic core" to being distinct hardware. '436 Patent at 10:58–61 ("the individual packet engines 228 may each independently process discrete packets and forward the packets to other devices, such as cryptographic processing cores or switches"); *see id.* at 11:11–16, 11:48–63 & 20:10–16. Defendants' proposal to limit a "cryptographic core" to being distinct, separate hardware is therefore hereby expressly rejected.

And here, too, surrounding claim language in Claims 1 and 13 of the ’436 Patent and Claims 1 and 13 of the ’612 Patent already recites the nature of the processing that the cryptographic core is configured to perform, namely “to provide encryption and decryption processing for packets received from and sent to the packet engine.” Defendants’ proposal is therefore redundant and would tend to confuse rather than clarify the scope of the claims.

The Court thus rejects Defendants’ proposed construction, but whereas Plaintiff proposes that no construction is necessary, “some construction of the disputed claim language will assist the jury to understand the claims.” *TQP*, 2012 WL 1940849, at *2.

The Court therefore hereby construes **“cryptographic core”** to mean **“hardware, or a combination of hardware and software, that is configured to perform cryptographic processing.”**

11. “intrusion detection system”

“intrusion detection system” (’436 Patent, Claims 1, 13; ’612 Patent, Claims 1, 13)	
Plaintiff’s Proposed Construction	**Defendants’ Proposed Construction**
No construction necessary. Plain and ordinary meaning. Alternatively, “hardware or microprocessor customized for matching parts of the data stream against the stored set of patterns”	“hardware customized for matching parts of the packet against the stored set of patterns in the signature database”

Dkt. No. 139, Ex. B at 12–13; Dkt. No. 149, Ex. A at 19.

Shortly before the start of the November 17, 2023 hearing, the Court provided the parties with the following preliminary construction: “hardware, software, or a combination thereof, that is configured for matching parts of a data stream against a stored set of patterns.”

(1) The Parties' Positions

Plaintiff argues that "[t]he '436 and '612 Patents expressly contemplate that the network intrusion detection functionality is not limited to hardware and may comprise 'firmware' and/or 'software' . . . ." Dkt. No. 145 at 20 (citing '436 Patent at 3:43–51, 12:2–5, 12:25–32, 12:66–13:5, 18:41–57 & 19:5–52). Plaintiff also argues that "Defendants' inclusion of the recited 'signature database' into the definition of 'intrusion detection system' imports additional limitations into the claim and otherwise confuses the Claims' discussion of the 'signature database.'" *Id.* at 21.

Defendants respond that "the specification never describes the IDS as a microprocessor," and "the portions of the specification relied on by Lionra relate[] to the functionality of the control processor and/or firmware, not the IDS, which is separately described." Dkt. No. 146 at 24 & 25 (citation omitted). Defendants also argue that "[t]he claims recite that the IDS is responsive to a 'packet matching a signature,'" and "[i]n order to be responsive to such a match, the IDS must be customized to perform such a matching of packets." *Id.* at 25. Finally, Defendants argue that "Defendants' construction provides necessary guidance as to where the 'set of patterns' is 'stored.'" *Id.*

Plaintiff replies that "Defendants do not point to any lexicography or disclaimer that requires limiting the 'intrusion detection system' to hardware," and "Defendants also fail to justify limiting the scope of the 'intrusion detection system' to require matching 'parts of the *packet*' (as opposed to the 'data stream')." Dkt. No. 148 at 8–9. Plaintiff also argues that "Claims 1 and 13 already delineate the relationship between the 'intrusion detection system' and 'signature database.'" *Id.* at 9.

At the November 17, 2023 hearing, Plaintiff agreed with the Court's preliminary construction. Defendants argued that software, by itself, would be insufficient.

<u>(2) Analysis</u>

Claim 1 of the '436 Patent, for example, recites (emphasis added):

> 1. A security processor to process incoming packets and outgoing packets, the security processor comprising:
>
> a switching system to send the outgoing packets and receive the incoming packets;
>
> a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system, wherein the packet engine is one of a plurality of packet engines and substantially all of the incoming packets and outgoing packets to the security processor transit one of the plurality of packet engines, and wherein the incoming packets and outgoing packets are provided with a tag upon ingress to one of the plurality of packet engines and the tag determines an egress path within the security processor upon exit from a corresponding cryptographic core;
>
> a cryptographic core, coupled to the packet engine and receiving the incoming packets from the switching system via the packet engine and communicating the outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core;
>
> a signature database; and
>
> an *intrusion detection system* coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database.

The specification discloses a "network intrusion detection system" ("NIDS"):

> NIDS 302 may flag a packet as having a potential signature match to a pattern in signature database 304. The flagged packet may either be dropped (and the flow of subsequent packets in the same data flow stopped) or continue to its next destination, with a logging report to host processor 130 in either case indicating the status of the packet. Also, in addition to being sent to its next destination, the flagged packet may be redirected or duplicated and receive further slow path processing by control processor 212. The logging report may be used to form an audit trail for collective or heuristic analysis and future packet inspection by a centralized intrusion detection system or other process or device. If a packet has been identified as undesirable, intrusion prevention may be provided by dropping related future packets in packet engines 228.

’436 Patent at 19:9–23; *see id.* at 19:5–52. The specification also discloses that intrusion detection functions can be implemented on processors:

> Control processor 212 and firmware 214 may provide all or substantially all control for these firewall, VPN and *network intrusion functions*.
>
> ***
>
> Other software stored as part of firmware 214 may be used to permit control processor 212 to provide VPN, firewall, *intrusion detection*/prevention, and SSL protocol communications, virus protection, digital rights management, content filtering, access control, verifying of application integrity, and management of public key infrastructure (PKI) exchanges.
>
> ***
>
> According to the present invention, by passing all I/O traffic to host processor 130 and/or internal network 116 through security processing system 102, and *including NIDS 302 within system 102*, undesirable intrusions may be detected in-line with such I/O traffic, such as, for example, it passes through an NIC [(Network Interface Card)]. By being in-line in this manner, intrusions identified by NIDS 302 may be stopped in the I/O traffic flow and any further related improper intrusion prevented from passing to host processor 130 and/or internal network 116.

’436 Patent at 12:2–5, 12:66–13:5 & 18:41–57 (emphasis added).

Thus, much like the “packet engine” and “cryptographic core” terms addressed above, the “intrusion detection system” can be implemented as hardware or a combination of hardware and software. As discussed regarding the term “packet engine,” the disclosure of an intrusion detection system as having “taps” (*id.* at 18:41–43) does not limit the term “intrusion detection system” to being a distinct physical structure. Defendants’ proposal to limit “intrusion detection system” to being distinct, separate hardware is therefore hereby expressly rejected.

Also, the parties agree that the intrusion detection system must be configured for “matching” parts of something “against the stored set of patterns,” but the parties disagree as to whether what is matched are parts of a “data stream” or parts of a “packet.” The claims and the specification refer to an intrusion detection system operating on "packets" (*see id.* at 19:5–52), but disclosure in the specification that an intrusion detection system "attempts to match parts of the *data stream* (for example, the header, payload, or trailer) against the stored set of patterns" is persuasive that the term "intrusion detection system" is not limited to packets. *Id.* at 18:45–47. Moreover, the specification expressly states that "as used herein, it is intended that the term 'packet' or 'packets' have the meaning and scope of the more generic term 'datagram' or 'datagrams.' *Id.* at 3:20–22.

Finally, Defendants' proposal of referring to a "signature database" is redundant because Claims 1 and 13 of the '436 Patent and Claims 1 and 13 of the '612 Patent already recite "matching a signature stored in the signature database." Defendants' proposal would therefore tend to confuse rather than clarify the scope of the claims.

The Court accordingly hereby construes **"intrusion detection system"** to mean **"hardware, or a combination of hardware and software, that is configured for matching parts of a data stream against a stored set of patterns."**

12. "security processor"

"security processor" ('436 Patent, Claim 1; '612 Patent, Claim 1)	
Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
Preamble not limiting. No construction necessary. Plain and ordinary meaning.	Preamble is limiting.

Dkt. No. 139, Ex. B at 15.

Plaintiff states: “In an effort to limit the number of disputes for the Court, Lionra agrees that the preamble language ‘security processor’ is limiting.” Dkt. No. 145 at 21.

The Court sets forth this agreement in Appendix A of this Claim Construction Order.

13. “security context management processing”

“security context management processing” (’436 Patent, Claim 2; ’612 Patent, Claim 2)	
Plaintiff’s Proposed Construction	**Defendants’ Proposed Construction**
No construction necessary. Plain and ordinary meaning. Not indefinite.	Indefinite.

Dkt. No. 139, Ex. B at 15; Dkt. No. 149, Ex. A at 24.

Shortly before the start of the November 17, 2023 hearing, the Court provided the parties with the following preliminary construction: “Plain meaning.”

(1) The Parties’ Positions

Plaintiff argues that “Defendants fail again to submit any evidence from a POSITA to support their indefiniteness position,” that “a POSITA understands that the recited ‘packet engine’ is configured to process information for managing the ‘security context’ of the incoming and outgoing packets,” and that the “security context” is a known term of art. Dkt. No. 145 at 22. Plaintiff also submits that these patents “provid[e] several examples of managing the security state of the incoming/outgoing packets.” *Id.* Finally, Plaintiff argues that Defendant Cisco “had no issue applying the term to the alleged prior art” in IPR petitions. *Id.* at 22–23.

Defendants respond that “[t]here is no dispute that ‘security context management processing’ is not a term of art,” and “[a]bsent an indication in the specification or file history as to how a packet engine 'handle[s] security context management processing,' this term is indefinite." Dkt. No. 146 at 26. Defendants also argue:

> Lionra's arguments should be rejected for additional reasons. First, like the phrase "security context management processing," the specification does not use the term "state of security," adding increased uncertainty to the scope of this claim. Second, the portions of the specification relied on by Lionra are generic discussions about the security processor, not specific functionality of the *packet engine* that performs the "security context management processing" in the claims. '436 Patent, 4:4–19. The functionality of the packet engine is specifically described in a separate portion of the specification not relied on by Lionra. *Id.*, 9:60–10:54. Third, the specification simply states the security processor may "maintain the relationships and integrity of the stored security context" and "store security associations." *Id.*, 4:4–15. At best, this describes storing "security context" or "security associations," not managing security context processing. Fourth, the specification uses the terms "state" and "context" distinctly. *Id.*, 5:32-35.

Dkt. No. 146 at 26–27 (footnote omitted).

Plaintiff replies that "[s]imply because the exact term 'security context management processing' is not used in the specification does not render Claim 2 indefinite," and "[t]he patents provide several examples of managing the security state of the incoming/outgoing packets." Dkt. No. 148 at 9 (citations omitted).

At the November 17, 2023 hearing, the parties reiterated the arguments set forth in their briefing.

(2) Analysis

As a threshold matter, the IPR proceedings cited by Plaintiff (*see* Dkt. No. 145 at 22–23) are unpersuasive because an IPR petition cannot assert indefiniteness. *See* 35 U.S.C. § 311(b); *see also Cuozzo Speed*, 136 S. Ct. at 2141–42.

Turning to the claim language, Claim 2 of the '436 Patent recites (emphasis added):

> 2. The security processor of claim 1 wherein the packet engine is further operable to handle *security context management processing* for the incoming and outgoing packets.

Defendants argue that Plaintiff's expert "does not cite to a single piece of evidence, intrinsic or extrinsic, in support" of Plaintiff's expert's opinion that "security context" is a known term of art. Dkt. No. 146 at 26. Plaintiff's expert opines:

> The '436 and '612 Patents . . . confirm that "security context" refers to the state of security for the in/out packets and that the packet engine is configured to handle or process information for managing the state of security (e.g. security context) of the packets, which information is stored in the memories.

Dkt. No. 145, Ex. 3, Sept. 1, 2023 Smith Decl. at ¶ 35 (emphasis omitted); *see id.* at ¶ 34 (citing '436 Patent at 4:5–19 & 5:32–35); *see also id.* at ¶ 33. Defendants present no evidence to rebut the opinion of Plaintiff's expert in this regard. Further, no internal inconsistency or inherent ambiguity is apparent in the claim language. Defendants do not meet their burden to show indefiniteness as to "security context management processing." *See Sonix*, 844 F.3d at 1377.

The Court therefore rejects Defendants' indefiniteness argument. Defendants present no alternative proposed construction, and no further construction is necessary.

The Court accordingly hereby construes **"security context management processing"** to have its **plain meaning**.

VI. DISPUTED TERMS IN U.S. PATENT NO. 7,916,630

The '630 Patent, titled "Monitoring Condition of Network With Distributed Components," issued on March 29, 2011, and bears an earliest priority date of September 16, 2004. The Abstract of the '630 Patent states:

> In a system having distributed components arranged in a logical ring structure, each component monitors only their respective neighboring component in the structure and the condition of the neighboring component is determined. If a component determines a condition of its neighboring component that corresponds to a predefinable condition, the component informs the other components of the system of the predefined condition of the neighboring component.

14. "leasing method"

"leasing method" ('630 Patent, Claim 3)	
Plaintiff's Proposed Construction	**Defendants' Proposed Construction**
No construction necessary. Plain and ordinary meaning. Alternatively, "a method whereby a component sends a message to or receives a message from a neighboring component, the absence of which forms the basis for assessing the current condition of the component sending the message"	"a method whereby a component sends a message to or receives a message from its neighboring component"[3]

Dkt. No. 139, Ex. B at 17.

Plaintiff submits in its reply brief: "In an effort to limit the number of disputes for the Court, Lionra agrees that the term 'leasing method' in Claim 3 of the '630 Patent means 'a method whereby a component sends a message to or receives a message from its neighboring component.'" Dkt. No. 148 at 10.

The Court sets forth this agreement in Appendix A of this Claim Construction Order.

[3] Defendants previously proposed: "a method whereby a component periodically sends an 'Alive' message to or receives an 'Alive' message from its neighboring component." Dkt. No. 139, Ex. B at 17.

15. “Inform All”

“Inform All” (’630 Patent, Claim 7)	
Plaintiff’s Proposed Construction	**Defendants’ Proposed Construction**
No construction necessary. Plain and ordinary meaning. Alternatively, “a method whereby a component informs other components regarding a condition of a neighboring component with a message”	“a method whereby a component informs all of the other components regarding a condition of a neighboring component with a message”

Dkt. No. 139, Ex. B at 18.

Plaintiff states: “In an effort to limit the number of disputes for the Court, Lionra agrees that the term ‘Inform All’ in Claim 7 of the ’630 Patent means ‘a method whereby a component informs all of the other components regarding a condition of a neighboring component with a message.’” Dkt. No. 145 at 25.

The Court sets forth this agreement in Appendix A of this Claim Construction Order.

VII. DISPUTED TERMS IN U.S. PATENT NO. 7,921,323

16. “said interconnection”

“said interconnection” (’323 Patent, Claim 28)	
Plaintiff’s Proposed Construction	**Defendants’ Proposed Construction**
Plain and ordinary meaning. No construction necessary. Not indefinite.	Indefinite

Dkt. No. 139, Ex. B at 19.

Plaintiff submits in its reply brief: “In an effort to limit the number of disputes for the Court and to further streamline the proceedings, Lionra is no longer asserting Claim 28 of the

’323 Patent against Defendants.” Dkt. No. 148 at 10. Because the claim in which the term “said interconnection” appears is no longer asserted, the Court does not further address this term.

VIII. CONCLUSION

The Court adopts the constructions set forth in this opinion for the disputed terms of the patent-in-suit.

The parties are ordered that they may not refer, directly or indirectly, to each other’s claim construction positions in the presence of the jury. Likewise, the parties are ordered to refrain from mentioning any portion of this opinion, other than the actual definitions adopted by the Court, in the presence of the jury. Any reference to claim construction proceedings is limited to informing the jury of the definitions adopted by the Court.

SIGNED this 27th day of November, 2023.

Roy S. Payne

ROY S. PAYNE
UNITED STATES MAGISTRATE JUDGE

APPENDIX A

Term	Parties' Agreement
"entity" ('708 Patent, Claims 1–2, 9–11)	"a user or process"
"access level" ('708 Patent, Claims 1–2, 9–11)	"a security level for access to a node"
"said request" ('708 Patent, Claims 1–2, 9–11)	"said access request"
"processing means" ('708 Patent, Claims 10, 11)	Means-plus-function term Function 1: "comparing said access request to said temporal access table to determine if said access request completes a prohibited temporal access pattern for said entity" Structure 1: computer system adapted to carry out the algorithms described in '708 Patent at 1:62–64; 5:33–35, Fig. 6; 5:36–37; 5:42–47; 5:54–56, Fig. 4B; 5:56–60, Fig. 3; 5:39–42, Fig. 6; 5:46–49; and equivalents thereof. Function 2: "comparing a minimum access level established for said first base node to said predetermined access level" Structure 2: computer system adapted to carry out the algorithms described in '708 Patent at Abstract; 1:65–67; 6:2–8; Fig. 6; and equivalents thereof. The elements recited in the "wherein" clause that follows are not functions, but rather further limits to the processor means element.
"arranged together with said base nodes in the form of a tree hierarchy" ('708 Patent, Claim 9)	The preamble language "arranged together with said base nodes in the form of a tree hierarchy" is limiting.

“security processor” (’436 Patent, Claim 1; ’612 Patent, Claim 1)	The preamble language “security processor” is limiting.
“leasing method” (’630 Patent, Claim 3)	“a method whereby a component sends a message to or receives a message from its neighboring component”
“Inform All” (’630 Patent, Claim 7)	“a method whereby a component informs all of the other components regarding a condition of a neighboring component with a message”

Dkt. No. 139, Ex. A; Dkt. No. 145 at 9, 21 & 25; Dkt. No. 146 at 6; Dkt. No. 148 at 10; Dkt. No. 149, Ex. A at 25–36.